陕西省交通运输厅

网络安全管理暂行办法

2019年1月

陕西省交通运输厅

## **第一章 总则**

1. 为加强陕西省交通运输厅网络安全管理，落实网络安全责任，提高网络安全保障工作水平，健全网络安全管理制度和运行安全机制，依据《中华人民共和国网络安全法》、国家有关法律法规和交通运输部网络安全有关规定，特制定本办法。
2. 陕西省交通运输厅网络安全工作按照“积极利用、科学发展、依法管理、确保安全”的方针和“同步规划、同步建设、同步使用”的要求，坚持“谁主管谁负责，谁运行谁负责”和“属地管理”原则，实行分级管理、分工负责。
3. 本办法适用于陕西省交通运输厅网络和信息系统的建设、运行、使用及监管等方面的安全管理。涉密信息系统网络安全管理，按照国家涉密信息系统相关规定执行。

## **第二章 安全职责**

1. 陕西省交通运输厅是陕西省交通运输网络安全工作主管部门，依法履行综合协调和指导监管职责：

（一）依照国家网络安全法律、法规和标准，编制厅网络安全规划、管理制度和规范，指导厅直各单位和处室开展网络安全工作；

（二）组织重大网络安全基础设施建设，研究解决涉及网络安全的重大事项；

（三）组织开展网络安全检查，配合交通运输部、省委网信办、省公安厅等部门开展网络安全工作，监督厅直各单位和处室履行、落实网络安全责任情况；

（四）指导和监督厅直各单位和处室开展等级保护、风险评估、关键信息基础设施的认定防护工作；

（五）建立陕西省交通运输厅网络安全监测预警、信息通报和应急处置机制，制定网络安全应急预案，通报网络安全信息，调查处理重大网络安全事件；

（六）组织开展网络安全宣传和培训工作。

1. 厅直各单位负责本单位网络安全工作，指导监管其下属单位开展网络安全工作，履行下列职责：

（一）执行国家和行业网络安全法律、法规与标准，编制本单位网络安全规划，制定本单位网络安全管理制度；

（二）落实网络安全等级保护制度，开展风险评估、安全自查等工作，加强关键信息基础设施的安全防护；

（三）加强网络安全监测预警，落实网络安全信息通报制度，制定本单位及下属单位网络安全应急预案，组织开展网络安全应急演练，采取有效措施，应对网络安全事件；

（四）配合上级网络安全管理部门进行网络安全检查和事件调查，对发现问题及时进行整改；

（五）组织开展本单位及下属单位网络安全宣传和培训工作。

1. 市交通运输主管部门在市委、市政府的领导下，贯彻落实国家、行业、地方相关网络安全法律法规和政策制度，负责本地区交通运输网络安全工作的综合协调和指导监管，配合省交通运输主管部门和市网信、公安等部门开展相关工作。
2. 陕西省交通运输厅网络安全和信息化领导小组是省厅网络安全和信息化工作管理机构，厅网信办是日常办事机构(设在厅科技处),承担网络安全管理日常工作；省交通运行监测中心受省厅委托行使网络安全管理职能；厅直各单位明确本单位网络安全管理部门，设置网络安全员专职岗位，落实网络安全责任制，其领导班子主要负责人是本单位网络安全工作的第一责任人。
3. 跨部门、跨层级的联网信息系统，应当划分网络安全管理边界，明确主管部门和相关运行单位安全管理责任，统一规划、统一建设、统一安全保护策略和统一监测管理，各自负责网络安全运行。

## **第三章 建设阶段安全**

1. 厅直各单位应当按照网络安全等级保护制度和规范要求，做好系统规划设计、建设开发、部署上线等环节的网络安全工作，建立覆盖系统建设各方、各环节的网络安全责任制。
2. 在信息系统可行性研究报告报审前，应当采取专家评审的方式确定安全保护等级，并严格按照所定级别设计安全建设方案。安全保护等级为第三级及以上的，安全设计方案应当通过专项评审。
3. 信息系统在建设、运行、使用及监管过程中，厅直各单位应当明确各参与方网络安全工作责任，签署相应的安全责任承诺书，报本单位网络安全管理部门备案。
4. 厅直各单位应当指定或授权专人负责产品采购，制定相应的管理制度对采购进行全程监督。安全产品和密码产品的选购，要选择符合国家及相关部门规定的产品。
5. 系统建设应当采取数据分类、数据备份和加密等措施，制定有效的数据备份和恢复策略，对重要网络设备和通信线路进行冗余备份，最大限度保障信息系统运行的连续性。
6. 对涉及行政许可、资金管理等业务的重要信息系统，应当采用陕西省交通运输密钥管理与安全认证中心密钥身份认证系统，实现双因子认证。
7. 厅直各单位应当与软件开发方签订相关安全和保密协议，按照安全需求及软件工程规范进行设计开发。对安全保护等级为第二级及以上系统，应当组织第三方专业机构开展软件测试、代码安全审计。未通过软件测试、代码安全审计的，应当在整改通过后方可投入试运行。试运行应当在测试环境中进行。
8. 安全保护等级为第二级及以上的新建系统投入试运行后30日内，向公安机关备案，并在备案完成后10日内将备案证明报备厅网信办。
9. 试运行期，对安全保护等级为第二级及以上系统，应当组织具备资质的第三方机构进行等级保护测评，对第三级及以上的系统，还应当组织开展风险评估。未通过等级保护测评及备案的，风险评估不合格的，应当在整改后开展竣工验收。
10. 建设单位与运行单位不是同一单位的，建设单位应当组织运行单位参与竣工验收，未通过等级保护测评及备案的，风险评估不合格的，未完成运行责任移交的，未完成设计、实施和开发技术文档及源代码等移交的，应当在整改后开展竣工验收。竣工验收完成后，由运行单位联系公安部门进行备案主体变更。
11. 系统功能发生重大变更时，厅直各单位应当组织重新定级，并根据定级结果重新组织评估系统安全防护能力，开展安全整改建设。

## **第四章 运行阶段安全**

#### 第一节 一般规定

1. 运行单位应当建立健全覆盖运行各环节的安全管理制度体系和操作规程，确定运行安全责任人，落实网络安全保护责任。
2. 运行单位应当建立人员录用、转岗和离岗以及外包服务人员等方面的安全管理制度，定期进行培训和考核，并签订安全保密协议。
3. 运行单位应当配备机房安全管理人员，严格机房出入安全管理，定期对机房开展检查，确保机房条件符合等级保护管理要求。
4. 运行单位应当对资产进行分类、标识，明确使用和处理措施，明确资产责任人，建立资产清单，并对存储介质和软硬件设备的采购、使用、存储、维护、报废等方面提出要求。对不满足安全管理规定的设备，按有关规定及时更新、报废。
5. 运行单位应当根据需求在不同网络间实行物理隔离或逻辑隔离，并按照最小权限原则对网络进行分区分域管理，在不同安全域间实施访问控制，严格控制非授权网络访问。加强对接入运行环境的行为严格管理，接入方案、安全测评报告等审核和评估后，确认达到安全要求方可授权接入，不得随意变更接入要求。
6. 运行单位应当对日常维护工作建立操作规程和巡检流程，指定专人对网络和系统的安全配置、日志审计等方面进行管理，划分系统管理员角色，明确各角色的权限及责任，定期开展漏洞扫描、恶意代码检测等工作，并及时整改，有效处置安全风险隐患。
7. 对安全保护等级为第三级及以上的系统，运行单位应当严格按照等级保护要求，每年至少开展一次等级符合性测评，并将测评报告报厅网信办备案。对未达到安全保护等级要求的及时开展安全整改。
8. 运行单位应当加强网站等互联网系统的安全防护，部署安全防护设备，严格设置访问控制策略，建立安全访问路径，严格控制后台维护终端的管理。
9. 运行单位应当加强互联网电子邮件系统安全管理。严禁将办公邮件自动转发至非相关人员或境外邮箱，确保用户密码具有一定强度并定期更换。加强人员安全意识教育，防止钓鱼邮件等网络攻击。
10. 运行单位应当采取技术措施监测、记录网络运行状态和网络安全事件，日志留存时间不少于六个月。
11. 运行单位应当建立变更管理制度，网络和系统发生重大变更时，应制定变更方案，并经过上级单位审批后，应按照既定的变更方案进行变更。
12. 运行单位应当建立备份与恢复安全管理制度，制订详细的备份与恢复策略和操作规程，对备份过程进行记录，定期执行恢复测试。
13. 国家重要活动、会议期间实行网络安全重点保障。厅直各单位应当按照“减风险，保关键”原则，做好事前检查和风险漏洞检测整改，加强重点防护并签署网络安全责任承诺书。实行专项信息通报，严格执行“零事件”报告制度。

#### 第二节 关键信息基础设施安全

1. 厅直各单位应当按照交通运输部关键信息基础设施相关认定规范进行系统梳理、初步认定，报厅网信办审核。
2. 关键信息基础设施采购可能影响国家安全的网络产品和服务，应当通过网络安全审查，并与供货方签订安全保密协议。
3. 关键信息基础设施运行单位应当设置专门安全管理机构，明确安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查，定期开展技术培训和技能考核。
4. 关键信息基础设施主管单位应当组织对关键信息基础设施实行7×24小时监测，每年至少组织开展一次风险评估。涉及密码应用的，每年至少组织开展一次密码应用安全性评估。
5. 关键信息基础设施收集和产生的个人信息和重要数据应当在境内存储，并对重要信息系统和数据进行容灾备份；因业务需要，确需向境外提供的，主管单位应当按照国家有关规定履行安全评估程序。严禁非法获取、出售或未经授权向他人提供关键信息基础设施技术资料。

## **第五章 信息数据安全**

1. 厅直各单位应当严格落实国家和行业对个人信息、重要数据保护的相关要求，遵循“谁收集信息、谁负责保护”的原则，组织建立健全用户信息保护制度，指导运行单位加强用户信息安全保障。
2. 收集、使用个人信息，应当遵循合法、正当、必要的原则，建立收集明示机制。明确数据公开收集和使用要求，规范采集、存储、使用、销毁等行为，严格限制对公民、法人和其他组织信息收集规模，不得收集与其提供的服务无关的个人信息；不得违反法律、行政法规规定和双方约定收集、使用、处理其存储的个人信息。
3. 厅直各单位应当采取必要措施，确保采集信息的安全，防止信息泄露、毁损、丢失。当发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
4. 跨部门、跨区域开展数据资源共享的系统，依据厅政务信息资源共享管理相关规定，加强数据安全管理。

## **第六章 信息通报与处置**

1. 厅直各单位应当加强网络安全监测预警能力建设，实时掌握网络安全态势，完善网络安全信息通报机制，加强网络安全信息收集、分析和共享，确保通报信息传达到位，及时开展通报预警风险核查处置，并按要求逐级反馈，不得瞒报、缓报、谎报、迟报和推诿责任。
2. 厅直各单位应当根据系统等级测评和风险评估结果，及时采取措施防范处置网络安全风险。
3. 厅直各单位应当加强风险漏洞管控，主动及时掌握网络产品和服务相关的安全信息，建立风险漏洞台账，履行整改第一责任。因技术条件限制，不能按期整改但需继续运行的，应当采取必要措施，避免发生安全事件，并以书面形式报备厅网信办。
4. 厅直各单位应当加强网络安全事件应急处置管理，明确应急工作机构，按照《陕西省交通运输厅网络安全事件应急预案（试行）》的要求，制定完善本单位网络安全事件应急预案，每年至少开展一次应急演练，并根据演练结果完善应急预案。
5. 厅直各单位应当制定安全事件报告和响应处置流程，明确安全事件类型及职责。网络安全事件发生后，应根据事件类型和级别，立即启动应急预案，最大程度减少损失和危害，及时开展信息通报，并向厅网信办上报。对处置过程进行记录，如可能涉及攻击、破坏等违法犯罪的，应当保护相关数据、记录、资料和现场，在24小时内向公安机关报案，并配合调查取证。
6. 网络安全事件处置完成后，应当及时完成网络安全事件调查和评估工作，对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

## **第七章 监督管理**

1. 厅网信办每年至少组织开展一次网络安全检查工作。根据国家有关要求，在重点保障时期对网络安全重点保卫单位开展专项检查。厅直各单位应当按要求组织开展自检自查工作，并配合上级网络安全管理部门做好网络安全检查工作。
2. 厅直各单位对检查过程中发现的问题应当限期完成整改，并将整改结果及时报厅网信办。
3. 厅直各单位网络安全主要负责人应当加强本单位网络安全工作的统筹管理，定期听取工作汇报、协调解决重大问题，组织落实机构、人员和经费等必要条件。
4. 厅直各单位应当将网络安全运行管理、教育培训、安全检查、测试评估、监测预警、应急处置等费用纳入年度预算，保障网络安全经费投入。
5. 厅直各单位应当组织开展网络安全教育工作，加强全员网络安全意识和知识技能培训。
6. 对违反本办法规定的，视情追究相关单位责任，由上级交通运输主管单位责令限期改正、暂停业务。逾期未改正的，给予通报批评，视情对主要负责同志进行约谈。情节严重并造成不良影响的，依照有关法律法规和网络安全工作责任制有关规定，启动问责程序，逐级倒查，追究当事人、网络安全负责人直至主要负责人责任，协调监管不力的，还应当追究综合协调或监管部门负责人责任。
7. 违反本办法规定，涉及使公民、法人或者其他组织的合法利益受到侵害的，依法承担民事责任；涉嫌违法犯罪的，移送公安机关处理。

## **第八章 附则**

1. 本办法相关术语含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指网络空间的安全，是通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）信息安全等级保护制度，是《网安法》规定的网络安全实行的管理制度，是指对国家秘密信息、法人或其他组织及公民专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级进行响应、处置。

（四）网络安全事件，是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为：信息内容安全事件、信息窃取事件、网络服务异常事件、有害程序事件、信息破坏事件、设备设施故障事件、灾害性事件和其他网络安全事件。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

（六）安全审计，是计算机网络安全审计的简称，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价。代码安全审计是检查[源代码](https://baike.so.com/doc/5395725-7589481.html%22%20%5Ct%20%22_blank)中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方。日志审计是记录与审查用户操作计算机及网络系统活动的过程，从而发现系统漏洞、入侵行为，是提高系统安全性的重要举措。

1. 本办法由厅网信办监督管理、修订完善及解释，厅直各单位和相关处室负责本办法的执行。
2. 本办法自发布之日起施行。